



US007307999B1

(12) **United States Patent**
Donaghey

(10) **Patent No.:** **US 7,307,999 B1**
(45) **Date of Patent:** **Dec. 11, 2007**

(54) **SYSTEMS AND METHODS THAT IDENTIFY
NORMAL TRAFFIC DURING NETWORK
ATTACKS**

2003/0097439 A1* 5/2003 Strayer et al. 709/224

(75) **Inventor:** **Robert J. Donaghey**, Lexington, MA
(US)

(73) **Assignee:** **BBN Technologies Corp.**, Cambridge,
MA (US)

(*) **Notice:** Subject to any disclaimer, the term of this
patent is extended or adjusted under 35
U.S.C. 154(b) by 1074 days.

(21) **Appl. No.:** **10/058,442**

(22) **Filed:** **Jan. 28, 2002**

Related U.S. Application Data

(60) **Provisional application No. 60/269,547**, filed on Feb.
16, 2001.

(51) **Int. Cl.**
H04J 3/16 (2006.01)

(52) **U.S. Cl.** **370/465; 370/389; 726/23**

(58) **Field of Classification Search** **370/235,**
370/252, 238, 410, 432, 401; 709/224, 240;
713/201, 162

See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

6,028,626 A	2/2000	Aviv	
6,321,338 B1	11/2001	Porras et al.	
6,484,203 B1	11/2002	Porras et al.	
6,578,147 B1	6/2003	Shanklin et al.	
6,816,973 B1*	11/2004	Gleichauf et al.	726/13
6,839,754 B2	1/2005	Nowak et al.	
6,850,491 B1*	2/2005	Firoiu et al.	370/235
6,880,090 B1*	4/2005	Shawcross	726/14
2002/0002686 A1*	1/2002	Vang et al.	713/201
2002/0032774 A1	3/2002	Kohler et al.	
2002/0035683 A1*	3/2002	Kaashoek et al.	713/154
2003/0051026 A1*	3/2003	Carter et al.	709/224

OTHER PUBLICATIONS

Glave, James, "Smurfing Cripples ISPs," Wired News, www.wired.com, 4 pages, Jan. 7, 1998.

Craig, Andrew, "Internet Gets Slammed By Widespread Attack," TechWeb, Technology News, www.techweb.com, 3 pages, Mar. 4, 1998.

Schuba et al. Analysis of a Denial of Service Attack on TCP. Proceedings of the 1997 IEEE Symposium on Security and Privacy. (1997).

(Continued)

Primary Examiner—Edan Orgad

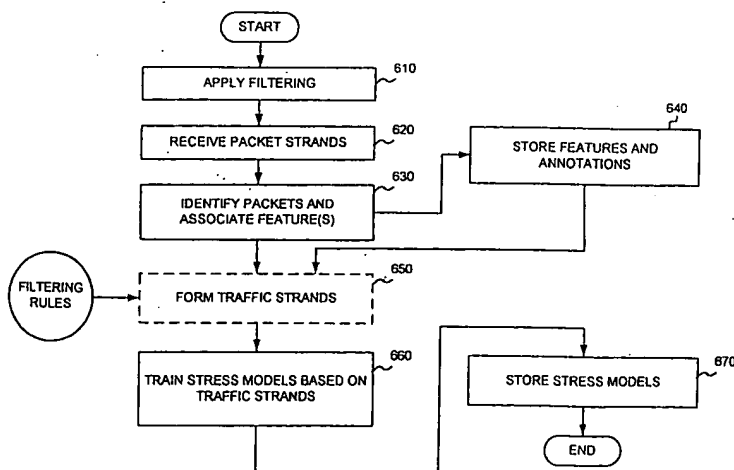
Assistant Examiner—Robert W. Wilson

(74) *Attorney, Agent, or Firm*—Ropes & Gray LLP

(57) **ABSTRACT**

A system protects against loss of communication during network attacks. In a first implementation, a system (120) models the behavior of normal users in a network in response to an application of a first packet filtering technique. The system (120) receives a group of packets from a first user subsequent to the application of the first packet filtering technique and creates one or more models reflecting the behavior of the first user based on the received packets. In another implementation, a system (130) receives a stream of packets subsequent to a filtering technique being applied, partitions the packets into groups, where each group corresponds to more than one packet, and classifies each group of packets as a normal group or an attack group using one or more models. Each model reflects a normal response to an application of the filtering technique. The system (130) forwards groups classified as normal groups, thus preventing network attacks from choking off all communication in the network.

17 Claims, 7 Drawing Sheets



OTHER PUBLICATIONS

Denning, Dorothy E. An Intrusion-Detection Model. IEEE Transactions on Software Engineering, pp. 118-131 (1987).

Jha et al. Markov Chains, Classifiers, and Intrusion Detection. Computer Security Foundations Workshop. Proceedings, 14th IEEE, pp. 206-219. (2001).

Vigna et al. NetSTAT: A Network-based Intrusion Detection Approach. ACSAC(1998).

Stallings, William. Cryptography and Network Security: Principles and Practice. 2nd ed., Prentice Hall, pp. 478-501 (1998).

* cited by examiner

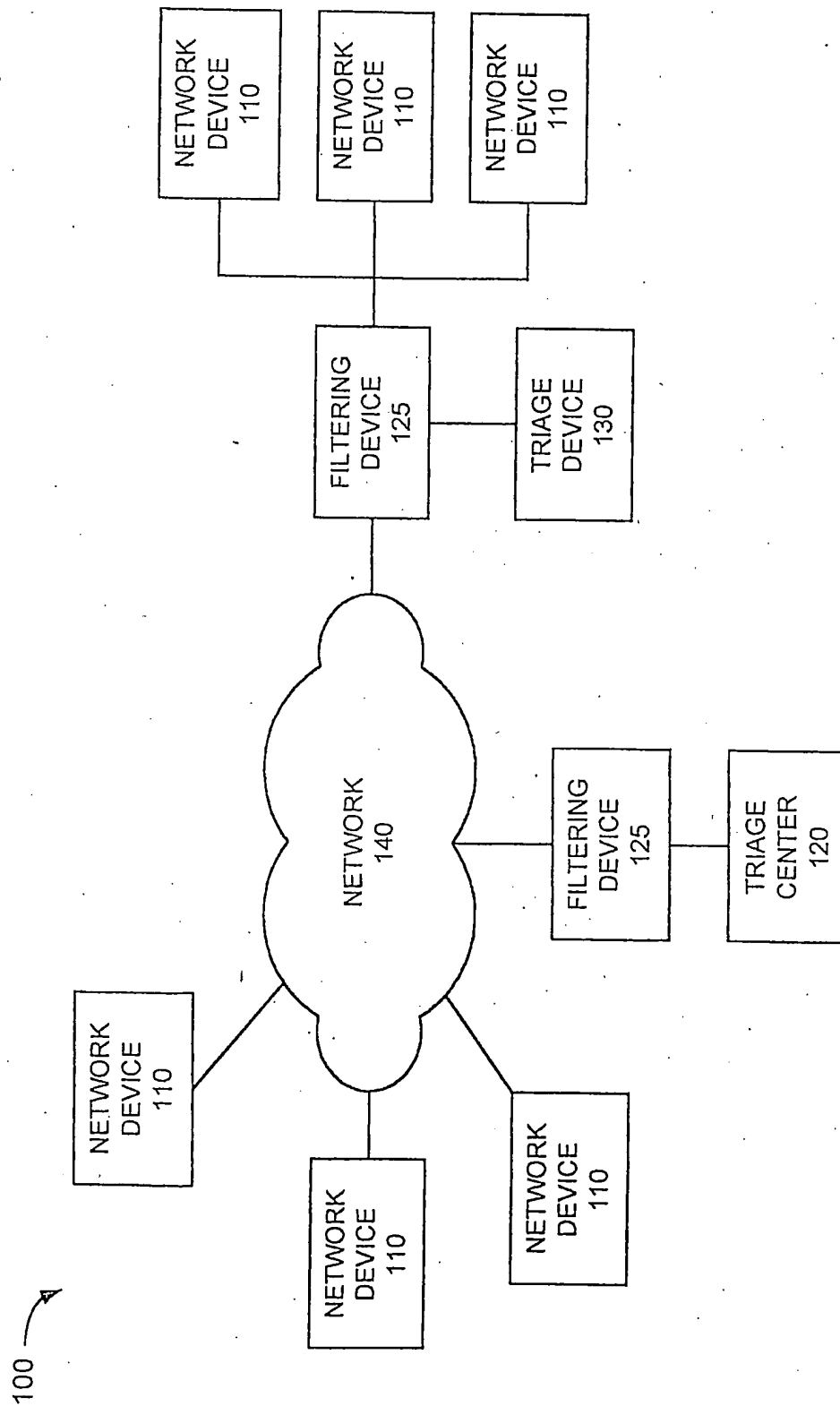


FIG. 1

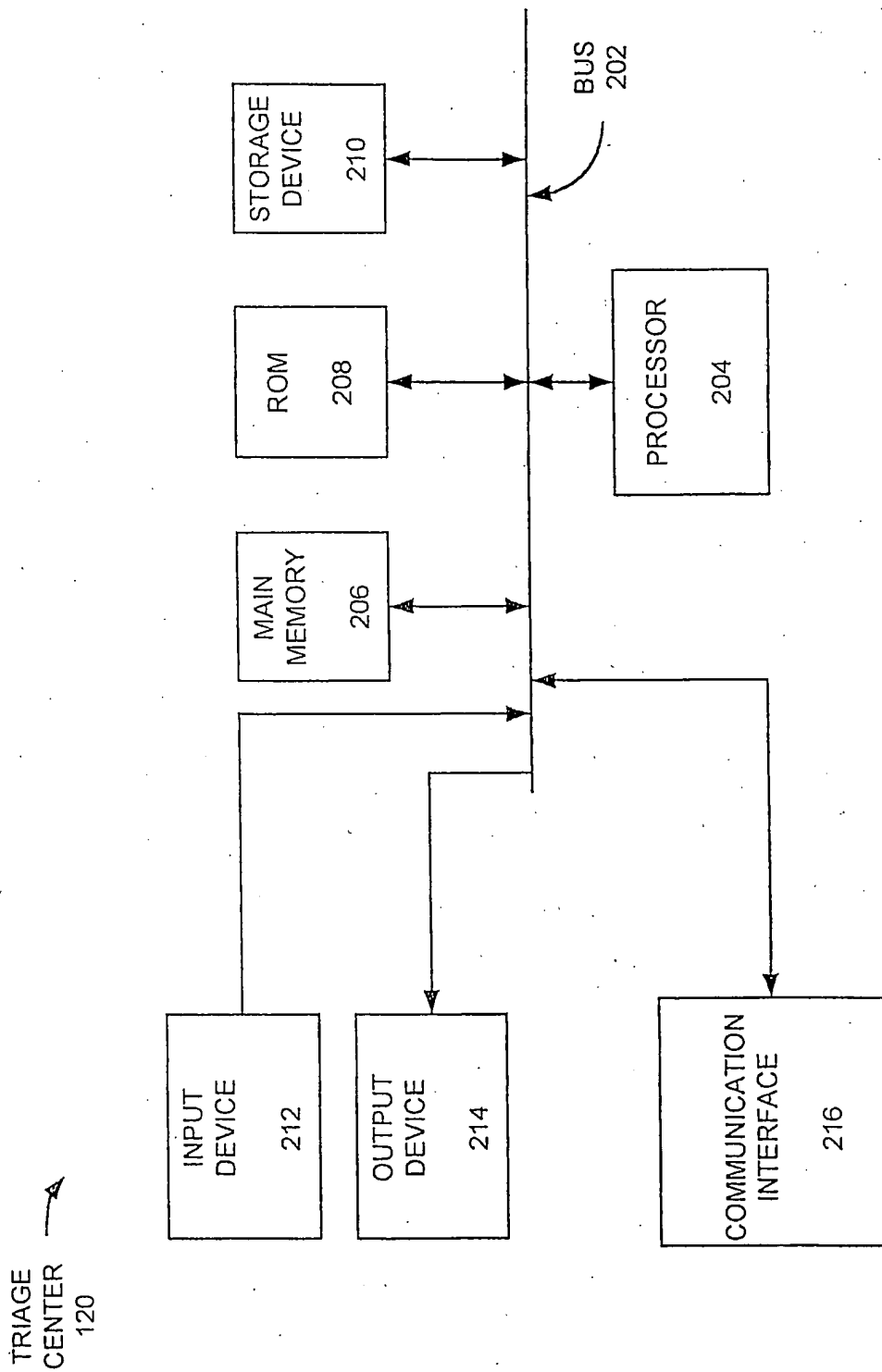


FIG. 2

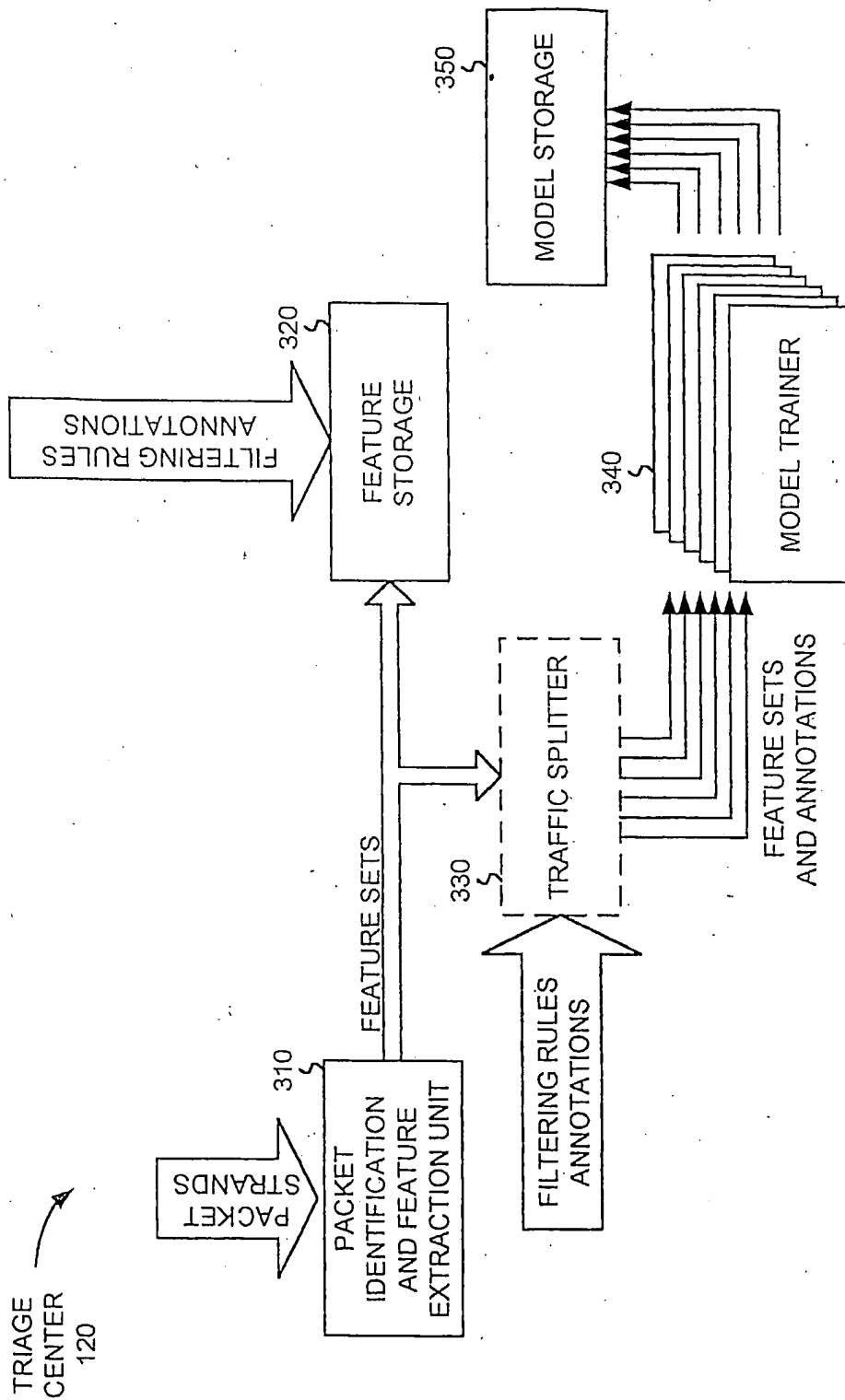


FIG. 3

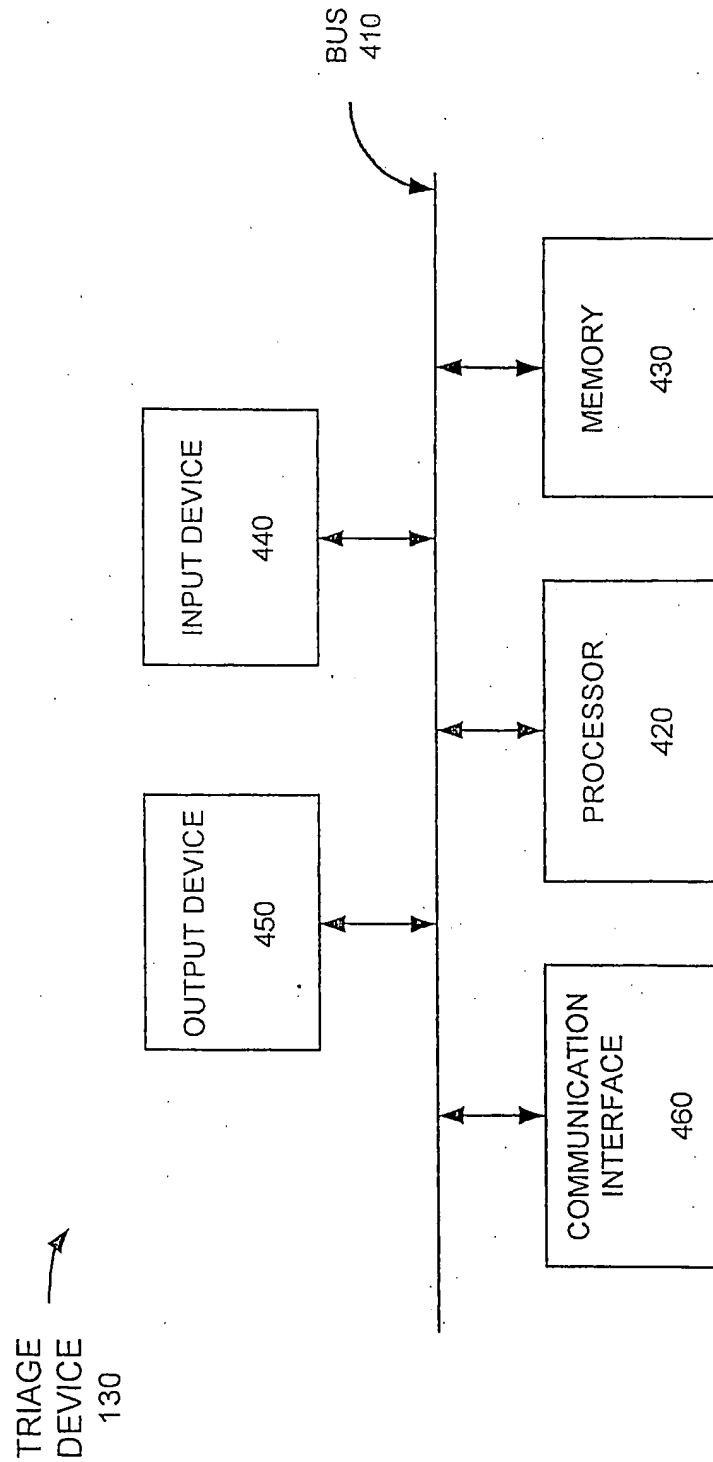


FIG. 4

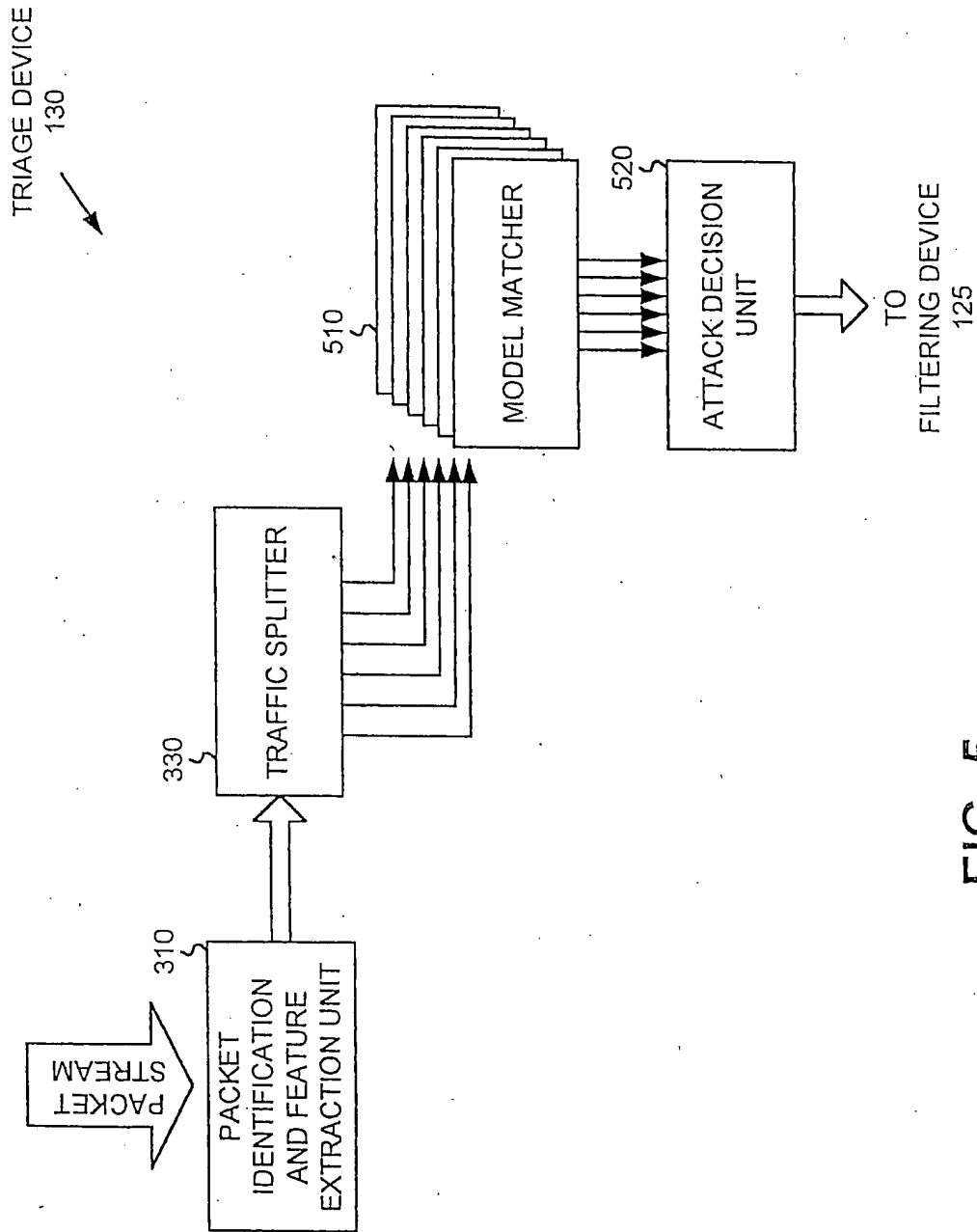


FIG. 5

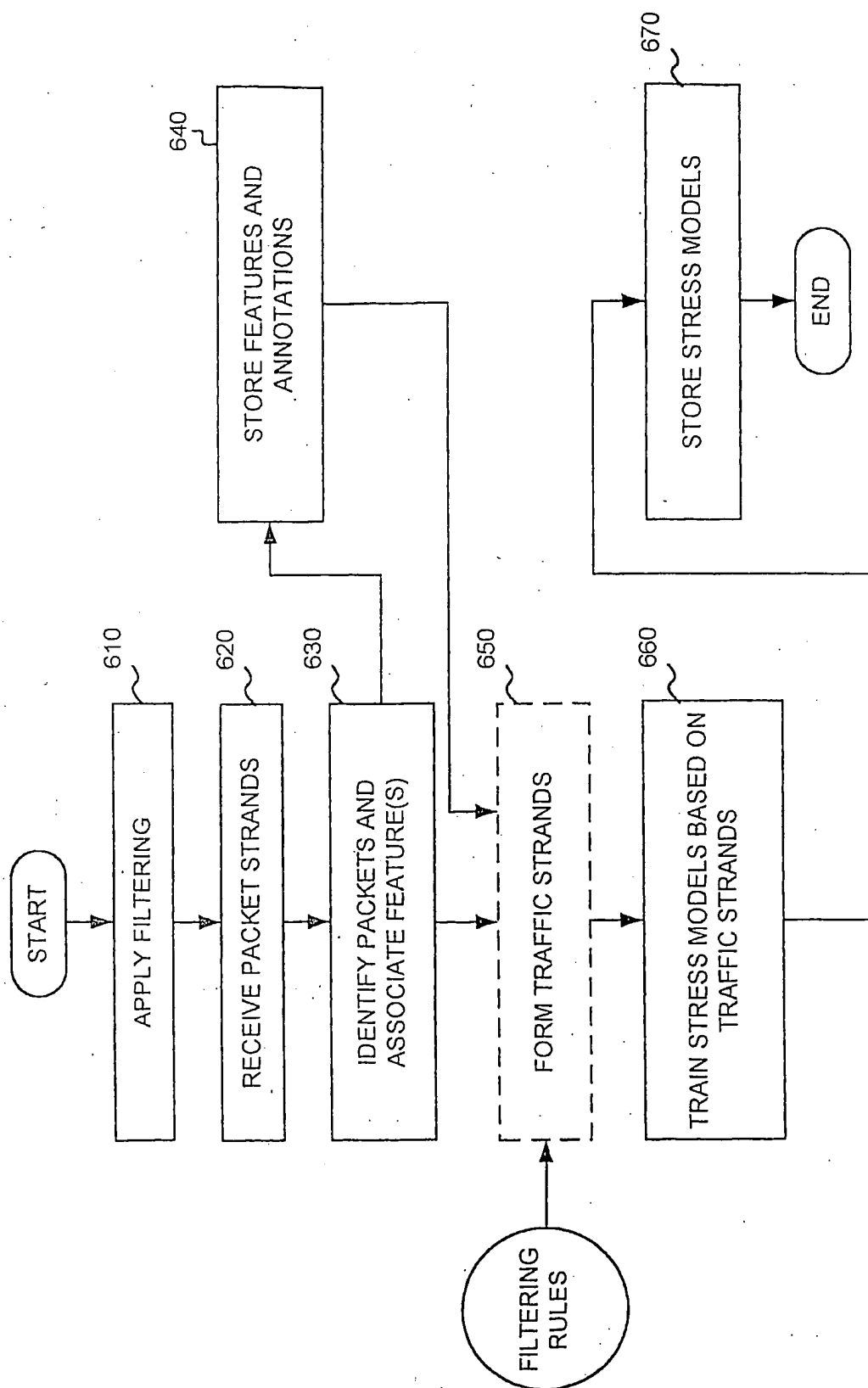


FIG. 6

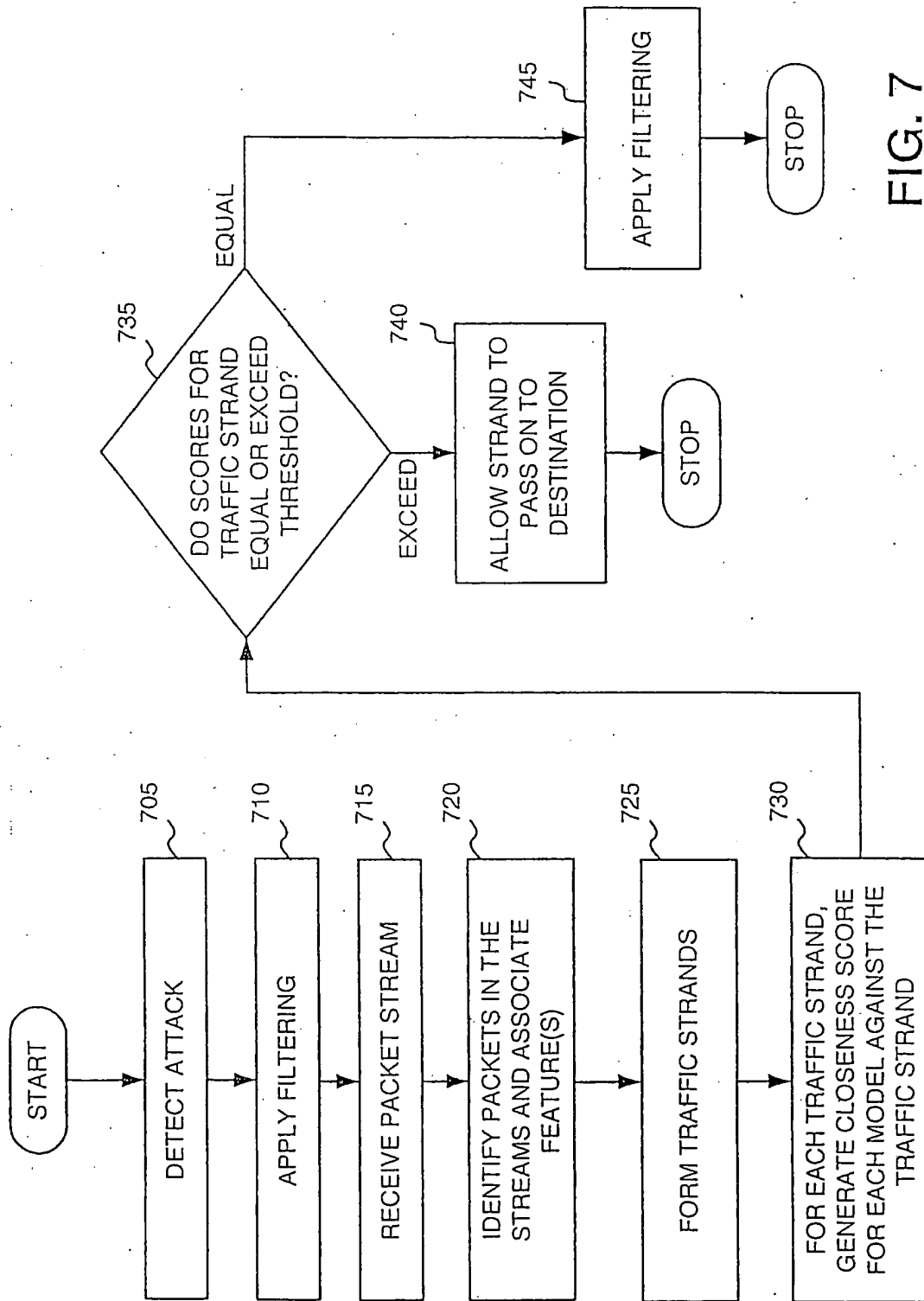


FIG. 7